Силабус курсу

УПРАВЛІННЯ ТА ЗАХИСТ ХМАРНИХ ІНФРАСТРУКТУР

Ступінь вищої освіти – магістр
Галузь знань – F Інформаційні технології
Спеціальність - F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Дисципліна циклу: вибіркова
Рік навчання: 1
Семестр: 2
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Тарас ЦАВОЛИК
Контактна інформація	tth@wunu.edu.ua

Опис дисципліни

Метою курсу вивчення дисципліни “Управління та захист хмарних інфраструктур” полягає у формуванні знань та навичок, для протидії сучасним кіберзагрозам через стрімке зростання використання хмарних технологій у всіх сферах бізнесу, державного управління та освіти. Хмарні сервіси стають основною інфраструктурою для зберігання, обробки та передачі даних, що супроводжується зростанням ризиків кіберзагроз, втрат даних, витоків інформації та атак на хмарні середовища.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
4/-	Вступ до хмарних обчислень та їх безпеки	Пояснювати різницю між сервісними та моделями розгортання хмарних середовищ. Аналізувати та застосовувати модель спільної відповідальності (Shared Responsibility Model) для різних хмарних сервісів. Визначати основні переваги та ризики використання хмарних технологій для бізнесу. Класифікувати ключові загрози безпеці у хмарних інфраструктурах.	Поточне опитування
2/-	Архітектура та компоненти хмарної інфраструктури	Принципи роботи технологій віртуалізації та контейнеризації. Розрізняти типи хмарних сховищ (об'єктні, блокові, файлові) та їх застосування. Пояснювати архітектуру програмно-визначених мереж (SDN) та їх роль у хмарі. Проєктувати базову архітектуру хмарного застосунку, обираючи відповідні компоненти.	Поточне опитування

2/-	Управління ідентифікацією та доступом (Identity and Access Management - IAM)	Налаштовування політики IAM на основі принципу найменших привілеїв (Principle of Least Privilege). Впроваджувати багатофакторну автентифікацію (MFA) для користувачів та сервісних акаунтів. Керувати життєвим циклом ідентичностей у хмарному середовищі. Інтегрувати хмарні сервіси з корпоративними системами ідентифікації.	Поточне опитування
2/2	Мережева безпека у хмарі	Проєктувати та створювати безпечну мережеву топологію в хмарі за допомогою VPC та підмереж. Налаштовувати правила фільтрації трафіку за допомогою груп безпеки та мережевих ACL. Розгортати та конфігурувати віртуальні брандмауери та VPN-з'єднання. Аналізувати мережевий трафік для виявлення аномалій та загроз.	Поточне опитування
2/2	Захист даних: шифрування та управління ключами	Застосовувати шифрування для різних типів хмарних сховищ та баз даних. Налаштовувати SSL/TLS для захисту даних під час передачі. Керувати ключами шифрування (створення, ротація, знищення) за допомогою Key Management Service. Обирати відповідний метод захисту (шифрування, токенізація) залежно від чутливості даних.	Поточне опитування
2/2	Безпека обчислювальних ресурсів	Застосовувати техніки "зміцнення" (hardening) для образів віртуальних машин та контейнерів. Налаштовувати автоматизоване сканування на вразливості та управління виправленнями. Ізолювати контейнерні застосунки для мінімізації поверхні атаки. Впроваджувати системи захисту кінцевих точок (Endpoint Protection) для хмарних ресурсів.	Поточне опитування
2/2	Моніторинг, логування та виявлення загроз	Налаштовувати централізований збір та аналіз логів (CloudTrail, Azure Monitor). Створювати панелі моніторингу (dashboards) для візуалізації стану безпеки інфраструктури. Налаштовувати правила оповіщення (alerts) для підозрілої активності. Інтегрувати хмарні логи з SIEM-системами для комплексного аналізу загроз.	Поточне опитування
2/2	Безпека додатків та DevSecOps	Інтегрувати інструменти сканування безпеки в конвеєр CI/CD. Аналізувати та усувати вразливості в коді додатків та їх залежностях. Впроваджувати заходи безпеки для API-шлюзів (автентифікація,	Поточне опитування, тестування

		авторизація, rate limiting). Оцінювати ризики безпеки для serverless-функцій (напр., AWS Lambda, Azure Functions).	
2/2	Реагування на інциденти та розслідування у хмарі	Розробляти план реагування на інциденти, адаптований до хмарної специфіки. Використовувати хмарні інструменти для збору та аналізу цифрових доказів (знімки дисків, логи). Виконувати процедури ізоляції скомпрометованих ресурсів для запобігання поширенню атаки. Проводити аналіз першопричин (root cause analysis) інциденту.	Поточне опитування
2/2	Комплаєнс та управління політиками в хмарі	Аналізувати вимоги основних стандартів безпеки та застосовувати їх до хмарної інфраструктури. Використовувати хмарні сервіси для проведення аудиту та моніторингу відповідності. Налаштовувати автоматизовані правила для запобігання порушенням політик безпеки. Готувати звітність щодо стану відповідності інфраструктури вимогам.	Поточне опитування
2/-	Автоматизація безпеки (Security Automation)	Писати безпечні шаблони IaC для автоматичного створення хмарних ресурсів. Впроваджувати перевірки безпеки в процес розгортання інфраструктури. Налаштовувати автоматизовані скрипти (напр., Lambda-функції) для реагування на події безпеки. Використовувати інструменти для автоматичного виправлення виявлених проблем конфігурації.	Поточне опитування
2/-	Управління станом безпеки хмари (Cloud Security Posture Management - CSPM)	Використовувати CSPM-інструменти для сканування хмарних середовищ на наявність ризиків. Інтерпретувати звіти CSPM та пріоритезувати виправлення на основі рівня ризику. Налаштовувати базові політики в CSPM-рішеннях. Пояснювати роль CSPM у підтримці безперервного комплаєнсу.	Поточне опитування
2/-	Відновлення після збоїв та безперервність бізнесу (DR/BCP)	Розробляти та тестувати план відновлення після збоїв (Disaster Recovery Plan). Налаштовувати автоматизоване резервне копіювання для різних типів даних. Проєктувати архітектуру, яка розподілена між кількома зонами доступності або регіонами. Розраховувати показники RTO (Recovery Time Objective) та RPO (Recovery Point Objective) для бізнес-процесів.	Поточне опитування
2/-	Просунуті загрози та методи захисту	Налаштовувати хмарні сервіси для захисту від DDoS-атак. Аналізувати тактики, техніки та процедури (TTPs), що	Поточне опитування

		використовуються APT-групами. Застосовувати сервіси аналітики загроз для проактивного виявлення шкідливої активності. Впроваджувати архітектурні патерни для зменшення ризиків від складних атак.	
2/-	Безпека мультихмарних та гібридних середовищ	Визначати основні проблеми безпеки в мультихмарних та гібридних архітектурах. Розробляти єдину стратегію управління ідентифікацією та доступом для різних середовищ. Використовувати інструменти для отримання централізованого огляду стану безпеки всієї інфраструктури. Планувати безпечне з'єднання між локальними дата-центрами та публічними хмарами.	Поточне опитування, тестування

Рекомендовані джерела інформації

1. Cloud infrastructure security: 10 key best practices. N-iX, 2024. Режим доступу: https://www.n-ix.com/cloud-infrastructure-security/ (переглянуто 2025).
2. Cloud Infrastructure Security: 7 Best Practices. Syteca, 2025. Режим доступу: https://www.syteca.com/en/blog/cloud-infrastructure-security (переглянуто 2025).
3. 9 Open source cloud security tools for 2025. Sysdig, 2025. Режим доступу: https://www.sysdig.com/blog/9-open-source-cloud-security-tools (переглянуто 2025).
4. What Is Cloud Infrastructure Security? Risks and Best Practices. LegitSecurity, 2025. Режим доступу: https://www.legitsecurity.com/aspm-knowledge-base/cloud-infrastructure-security (переглянуто 2025).
5. Top 10 Cloud Security Tools for 2025. Jit.io, 2024. Режим доступу: https://www.jit.io/resources/cloud-sec-tools/cloud-security-tools-for-2023 (переглянуто 2025).
6. Cloud Threats on the Rise: Alert Trends Show Intensified Attacks. Palo Alto Networks Unit42, 2025. Режим доступу: https://unit42.paloaltonetworks.com/2025-cloud-security-alert-trends/ (переглянуто 2025).
7. Cloud computing trends for 2023 - 2025. Nearshore, 2024. Режим доступу: https://nearshore-it.eu/technologies/cloud-computing-trends-for-2023-2025/ (переглянуто 2025).
8. 20 Cloud Security Best Practices. CrowdStrike, 2024. Режим доступу: https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-security-best-practices/ (переглянуто 2025).
9. Top 7 Cloud Security Frameworks and How to Choose. Exabeam, 2025. Режим доступу: https://www.exabeam.com/explainers/cloud-security/top-7-cloud-security-frameworks-and-how-to-choose/ (переглянуто 2025).
10. What is Cloud Risk Management?. Orca Security, 2024. Режим доступу: https://orca.security/resources/blog/what-is-cloud-risk-management/ (переглянуто 2025).
11. What is Cloud Infrastructure Security?. SentinelOne, 2025. Режим доступу: https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-infrastructure-security/ (переглянуто 2025).
12. Cloud Security Risks: What to Look Out for and How to Stay Safe. Gigacloud, 2025. Режим доступу: https://gigacloud.ua/en/articles/ryzyky-hmarnoyi-bezpeky-na-shho-zvernuty-uvagu-ta-yak-zahystytysya/ (переглянуто 2025).
13. Cloud Security Best Practices: 22 Steps for 2025. Wiz.io, 2024. Режим доступу: https://www.wiz.io/academy/cloud-security-best-practices (переглянуто 2025).
14. A Guide to Cloud Security Frameworks. Sangfor, 2024. Режим доступу: https://www.sangfor.com/blog/cloud-and-infrastructure/guide-to-cloud-security-frameworks

(переглянуто 2025).
15. How to Perform a Cloud Risk Assessment. Cymulate, 2025. Режим доступу: https://cymulate.com/blog/cloud-risk-assessment/ (переглянуто 2025).

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами освіти і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу учасник може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими учасниками, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Оцінювання

Підсумковий бал (за 100-бальною шкалою) з дисципліни Управління та захист хмарних інфраструктур» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Визначається як середнє арифметичне з оцінок отриманих на заняттях.	Модульна робота.	Оцінка за виконання та презентацію завдання тренінгу.	Оцінка за виконане завдання самостійної роботи.	Теоретичні питання: 1 питання - max 40 балів. 2 практичних завдання по 30 балів - max 60 балів

Шкала оцінювання

За шкалою університету	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	**A** (відмінно)
85–89	добре	**B** (дуже добре)
75–84		**C** (добре)
65–74	задовільно	**D** (задовільно)
60–64		**E** (достатньо)
35–59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1–34		**F** (незадовільно з обов'язковим повторним курсом)